AMENDMENTS TO THE CLAIMS

1. (Currently amended) A security document, comprising a printed document and one or more memory circuits ~~which is~~ configured to be read wirelessly and ~~which is~~ attached to or incorporated within the printed document, wherein data in the memory circuit is protected from access by an unauthorised reader, and wherein the memory circuit is physically isolated so as to inhibit physical tampering or is configured to indicate when physical tampering has occurred.

2. (Original) A security document as claimed in claim 1, wherein the memory circuit is inductively powered.

3. (Original) A security document as claimed in claim 2, wherein the memory circuit receives and transmits data wirelessly at radio frequency.

4. (Previously presented) A security document as claimed in claim 1, wherein physical isolation of the memory circuit employs one or more tamper-evident strips.

5. (Previously presented) A security document as claimed in claim 1, wherein an antenna of the memory circuit is configured for detection or resistance of physical tampering.

6. (Previously presented) A security document as claimed in claim 1, wherein the security document is configured to identify an authorised bearer of the security document.

7. (Previously presented) A security document as claimed in claim 6, wherein the security document is configured to allow access to a specified asset or assets by the authorised bearer.

8. (Currently amended) A method of publishing a security document, comprising:

a. determining first information for printing in a printed document, and second information for writing to one or more memory circuits for attachment to or incorporation within the printed document;
b. protecting the second information from unauthorised reading;
c. printing the first information in the printed document;
d. writing the second information to one or more memory circuits configured to be read wirelessly for attachment to or incorporation within the printed document; and
e. physically isolating the one or more memory circuits so as to inhibit physical tampering or configuring the one or more memory circuits to indicate when physical tampering has occurred.

9. (Original) A method of reading a security document comprising a printed document and one or more memory circuits attached to or incorporated within the printed documents, comprising:

f. obtaining authorisation information to read the security document;
g. reading first information printed in the printed document;
h. wirelessly powering at least one memory circuit and wirelessly reading protected second information stored in said memory circuit;
i. reading the second information by using the authorisation information; and
j. using the second information with the first information to assess the security document.

10. (Original) A method as claimed in claim 9, further comprising comparing the second information to one or more characteristics of a bearer of the security document.

11. (Previously presented) A security document, comprising a printed document and one or more memory circuits configured to be read wirelessly attached to or incorporated within the printed document, wherein data in the memory circuit is protected from access by an unauthorised reader, wherein the memory circuit is physically isolated so as to inhibit physical tampering or is configured to indicate when

physical tampering has occurred, and wherein both printed data and data in the memory circuit is configured to identify a bearer of the security document.

12. (Previously presented) A method of publishing a security document for a bearer, comprising:

k. determining first information concerning the bearer for printing in a printed document, and second information concerning the bearer for writing to one or more memory circuits for attachment to or incorporation within the printed document;

l. protecting the second information from unauthorised reading;

m. printing the first information in the printed document;

n. writing the second information to one or more memory circuits configured to be read wirelessly for attachment to or incorporation within the printed document; and

o. physically isolating the one or more memory circuits in the printed document so as to inhibit physical tampering or to indicate when physical tampering has occurred.